LETTER

Secure Handover Protocol for Mobile WiMAX Networks

Song-Hee LEE[†], ***Student Member***, **Nam-Sup PARK**[††], ***and*** **Jin-Young CHOI**[†a)], ***Nonmembers***

SUMMARY In this paper, we analyze existing vulnerabilities in handover for mobile WiMAX networks. To overcome these vulnerabilities, we propose a secure handover protocol that guarantees mutual authentication and forward/backward secrecy in handover. We present a formal analysis of our protocol using a logic-based formal method.

key words: *secure handover, mobile WiMAX, IEEE 802.16e, cross function*

1. Introduction

WiMAX (Worldwide interoperability for Microwave Access) is a wireless broadband technology based on the IEEE 802.16 family of standards [1]. The latest version of IEEE 802.16e, which is a revision of IEEE 802.16-2004, supports the mobility of a mobile station (MSS) [1]. For fast handover, IEEE 802.16e supports optimized handover that can omit some or all messages usually required in handover. Especially, Privacy Key Management (PKM) authentication and Traffic Encryption Key (TEK) handshake can be omitted, with different security settings for handover optimization; Bit #1 and #2 in the Ranging Response (RNG-RSP) message. Unfortunately, this can obviously lead to vulnerabilities in authentication and forward/backward secrecy. Although PKM authentication and TEK handshake are performed in handover, PKM authentication in the standard may not be suitable for fast handover, since PKM authentication, which is based on Extensible Authentication Protocol (EAP), can increase the handover delay. Also, TEK in the IEEE 802.16e standard is randomly generated by the Base Station (BS) and directly used for encryption. This design, however, provides insufficient security, because it is completely dependent on a single participant. Consequently, a means of providing secure handover in mobile WiMAX networks is needed.

Recent studies [4], [5] have proposed a secure and fast handover scheme for broadband wireless networks. In [4], it was shown that there is a cross-layer design for fast and secure handover, which is a combination of a MAC layer handover and an FMIP handover at the IP layer. This protocol involves designing a cross-layer and cross-function, to improve the handover latency of broadband wireless networks. Unfortunately, this work merely elaborated on the means of reducing the re-authentication time, and provided an analysis of the handover delay. In [5], secure handover authentication is based on a combination of pre-authentication and the PKI architecture. However, this method can result in unnecessarily power expenditure in key exchange, and vulnerabilities.

In this paper, we propose a secure handover protocol for mobile WiMAX networks. To overcome existing vulnerabilities, PKM authentication and TEK handshake are modified and combined with handover signaling, for fast handover. Unlike some previous studies, we focus on security. The purpose of the protocol is to provide mutual authentication and forward/backward secrecy via design of a cross-function. The proposed protocol securely establishes a unique authorization key (AK) and traffic encryption key (TEK) in the MSS and target base station (BS), in pre-authentication between the BSs and the authentication server (AS). By avoiding sharing of secret information between BSs, forward secrecy and backward secrecy are guaranteed. Finally, we present a formal analysis of our protocol, using a logic-based formal method.

The remainder of this paper is organized as follows. In Sect. 2, we propose a secure handover protocol in mobile WiMAX. We analyze a correctness proof of our protocol using a formal method, and security, in Sect. 3 and Sect. 4, respectively. Finally, Sect. 5 presents our conclusion.

2. Secure Handover Protocol for Mobile WiMAX

In this section, we introduce the proposed secure handover protocol for mobile WiMAX. The details of the protocol are depicted in Fig. 1. We use the notation summarized in Table 1 to describe our protocol.

2.1 Security Requirements

The security requirements for secure handover are summarized below:

- *Mutual authentication*: Mutual authentication between an MSS and a target BS must be provided, as a measure of trust. Via mutual authentication, various types of attacks on the MSS and the target BS, such as the replay attack and man-in-the-middle attack, can be prevented.
- *Forward secrecy and backward secrecy*: Previous security keys shared by the MSS and the serving BS must

Manuscript received June 19, 2008.
Manuscript revised August 26, 2008.

[†]The authors are with the Department of Computer Science and Engineering, Korea University, Korea.
[††]The author is with LG Electronics Inc., 219–24, Gasan-dong, Gumchon-gu, Seoul, Korea.
a) E-mail: choi@formal.korea.ac.kr

DOI: 10.1093/ietisy/e91–d.12.2875

Table 1 Notation.

Notation	*Description*
M, S, T, AS	The IDs of MSS, Serving BS, Target BS and Authentication Server, respectively
N_M	Nonce generated by MSS
$+K_M$	Public key of MSS
$-K_M$	Private key of MSS
$\{X\}\{+K_M\}$	X is encrypted by public key of MSS.
$\{X\}\{-K_M\}$	X is encrypted by private key of MSS.
H ()	One-way hash function
HMAC/CMAC	Message authentication codes
|	Concatenation operator

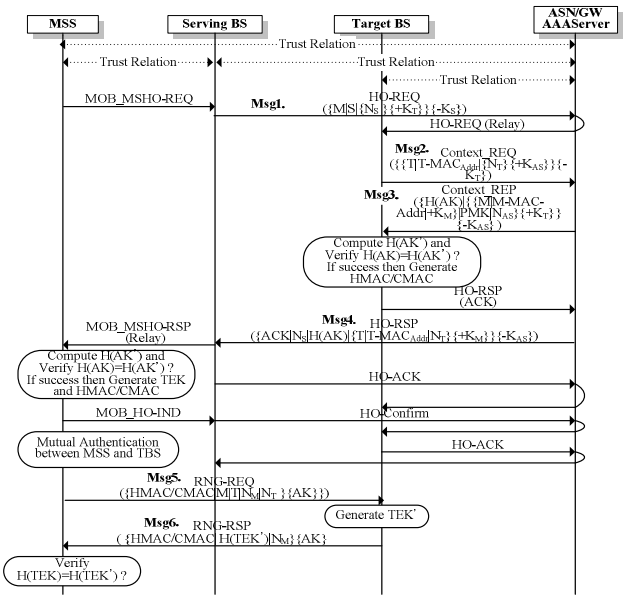

Fig. 1 Secure handover protocol.

be hidden from a target BS. Any new security keys shared by the MSS and the target BS must be hidden from the serving BS, after the handover.

2.2 Protocol Design

Figure 1 shows the secure handover protocol for IEEE 802.16e mobile WiMAX. Prior to the handover, trust relations should be established, which are based on pre-authentication, as shown in Fig. 1. Our protocol can satisfy security requirements via the modification of PKM authentication and TEK handshake, instead of additional EAP based re-authentication.

As shown in Fig. 1, our proposed protocol consists of a six-way handshake for re-authentication. The purpose of the four messages (Msg1–Msg4.) is to distribute keying parameters, to generate an AK (Authorization Key), and verify the correctness of the AK. In this phase, an AS (Authentication Server) generates a unique PMK and AK, which binds the identification of the target BS and the MSS, and securely delivers the hash value of the AK, the PMK (Pairwise Master Key), and its keying parameters to the corresponding BS, instead of the MSK (Master Session Key). Unlike the standard method, since the PMK is not shared with other BSs, other BSs can not derive the AK. Hence, forward/backward secrecy is guaranteed. Equivalently, a PMK and AK are generated by a target BS and an MSS. PMK generation is modified as follows:

$$PMK = Dot16KDF(MSK, \quad BSID \mid M - MAC_{Addr} \mid "PMK", 160), \qquad (1)$$

Where the Dot16KDF algorithm is a CTR (counter) mode construction that may be used to derive an arbitrary amount of keying material from source keying material [1]. BSID denotes the identification of the BS and $M\text{-}MAC_{Addr}$ denotes the MAC address of the MSS.

In order to support mutual authentication between an MSS and a target BS, two messages (Msg5 and Msg6) exchange HMAC/CMAC codes, then generate a TEK (Traffic Encryption Key) at the target BS and the MSS, respectively. To provide additional security, TEK generation was modified as follows:

$$TEK = PRF(N_M \mid N_T \mid M{-}MAC_{Addr} \mid T{-}MAC_{Addr}), \qquad (2)$$

Where PRF is a pseudo-random number function that produces a sequence of values based on a seed and current state. Given identical seeds, a PRF always outputs an identical sequence of values [6]. MAC addresses provide unique information and are securely exchanged via previous messages.

In summary, since the modification of PKM authentication can lead to generation of a unique PMK and AK, without additional EAP re-authentication, neighbor BSs cannot derive keys. Therefore, forward/backward secrecy is guaranteed in the proposed protocol. In addition, the modification of TEK can enhance security, as well as reduce the SA-TEK three-way handshake phase.

3. Formal Analysis Using GNY Logic

In this section, we describe a formal analysis of the proposed six-way handshake based on GNY logic [7], [8]. GNY logic is commonly used to analyze the security of cryptographic protocols. All symbols, notation and rules are cited in [7], [8].

3.1 Formalized Protocol

The conventional notation used in a generic protocol is not suitable for logical manipulation. Therefore, we formalized the six-way handshake of the proposed protocol for verification, as shown in Table 2. (Refer to Appendix A for the detailed notation)

The initial assumptions of the proposed scheme are as follows:

(A1) $M \ni N_M$, (A2) $M \mid\equiv \#N_M, \#N_T$, (A3) $T \ni N_T$,

Table 2 Formalized protocol.

Msg1.	$T \lhd *(\{M \mid S \mid \{*N_S\}\{+K_T\}\}\{-K_S\})$
Msg2.	$AS \lhd *(\{*\{T \mid *T-MAC_{Addr} \mid \{*N_T\}\{+K_{AS}\}\}\{-K_T\})$
Msg3.	$T \lhd *(\{*\{*H(AK) \mid *\{\{M \mid M-MAC_{Addr} \mid +K_M\} \mid *PMK \mid N_T \mid *N_{AS}\}\{+K_T\}\}\{-K_{AS}\})$
Msg4.	$M \lhd *(\{N_S \mid *H(AK) \mid *\{*T \mid *T-MAC_{Addr} \mid *N_T\}\{+K_M\}\}\{-K_{AS}\})$
Msg5.	$T \lhd *(\{*HMAC/CMAC \mid M \mid T \mid *N_M \mid N_T\}\{AK\})$
Msg6.	$M \lhd *(\{*HMAC/CMAC \mid *H(TEK') \mid N_M\}\{AK\})$

(A4) $T \mid\equiv \#N_T, \#N_S, \#N_{AS}, \#N_M$, (A5) $S \ni N_S$,
(A6) $S \mid\equiv \#N_S$,
(A7) $AS \ni N_{AS}$, (A8) $AS \mid\equiv \#N_{AS}, \#N_T$,
(A9) $M \ni +K_M, -K_M, \{M, +M_T\}$,
(A10) $T \ni +K_T, -K_T, \{T, +K_T\}, \{S, +K_S\}, \{AS, +K_{AS}\}$,
(A11) $S \ni +K_S, -K_S, \{S, +K_S\}, \{T, +K_T\}, \{M, +K_M\}, \{AS, +K_{AS}\}$,
(A12) $AS \ni +K_{AS}, -K_{AS}, \{AS, +K_{AS}\}, \{S, +K_S\}, \{T, +K_T\}, \{M, +K_M\}$,
(A13) $M \ni PMK$, (A14) $S \ni PMK$, (A15) $AS \ni PMK$,
(A16) $M \ni M-MAC_{Addr}$, (A17) $AS \ni M-MAC_{Addr}$,
(A18) $T \ni T - MAC_{Addr}$,
(A19) $M \ni HMAC/CMAC$, (A20) $T \ni HMAC/CMAC$

The assumptions describe the possessions and beliefs of both principals. Assumptions (A1–A8) imply that each principal not only possesses their own nonce, which it believes to be fresh, but also believes that the other principal's nonces are fresh. Assumptions (A9–A15) imply that the principals possess their own public key pairs and certificates, based on pre-authentication. Assumptions (A16–A18) imply that both the MSS and the target BS know their own MAC addresses, and the AS knows the MAC address of the MSS, via the previous authentication between the MSS and the serving BS. The last two assumptions (A19–A20) imply that the message authentication codes (HMAC/CMAC) are derived from the AK, at the MSS and the target BS, respectively.

3.2 Analysis of Correctness Proofs

Msg1 in our six-way handshake and Assumption A10 yield the following equations, from the application of rules T1, T4, and T6. (Refer to Appendix B)

$$\frac{T \lhd *(\{M \mid S \mid \{*N_S\}\{+K_T\}\}\{-K_S\}),\ T \ni +K_S}{T \lhd (M \mid S \mid \{N_S\}\{+K_T\})}(\text{T1, T4}) \tag{3}$$

$$\frac{T \lhd (M \mid S \mid \{N_S\}\{+K_T\}),\ T \ni -K_T}{T \lhd (M \mid S \mid N_S)}\ (\text{T6}) \tag{4}$$

The application of rules P1, and P3, yields:

$$\frac{T \lhd M \mid S \mid *N_S}{T \ni N, S, N_S}\quad (\text{P1, P3}) \tag{5}$$

The Application of A4 and rules F1, yields:

$$\frac{T \mid\equiv \#(N_S)}{T \mid\equiv (N, S, N_S)}\quad (\text{A4, F1}) \tag{6}$$

The target BS possesses the nonce generated by the serving BS. A nonce that is included in data exchanged by a protocol is usually used to guarantee freshness, and protect against replay attacks. Therefore, the target BS believes that the message is fresh.

Msg2, and Assumptions A8, A10 and A12, yield the following equations, from the application of rules T4, T6, P1, and P3:

$$\frac{AS \lhd *(T \mid *T - MAC_{Addr} \mid *N_T)}{AS \ni T, T - MAC_{Addr}, N_T} \tag{7}$$

$$\frac{AS \mid\equiv \#(N_T)}{AS \mid\equiv \#(T, T - MAC_{Addr}, N_T)} \tag{8}$$

The AS possesses the ID of the target BS, the MAC address of the target BS, and the nonce generated by the target BS, and believes in the freshness of the message. Then, the AS can generate the AK for the MSS and the target BS.

$$\frac{T \lhd *H(AK) \mid *\{M \mid M-MAC_{Addr} \mid +K_M\} \mid *PMK \mid N_T \mid *N_{AS}}{T \ni H(AK), N, M-MAC_{Addr}, +K_M, PMK, N_{AS}} \tag{9}$$

$$\frac{T \mid\equiv \#(N_T)}{T \mid\equiv \#(H(AK), M, M-MAC_{Addr}, +K_M, PMK, N_T, N_{AS})} \tag{10}$$

Msg3, and Assumptions A4, A10 and A12, yield Eqs. (9), (10), from the application of rules T4, T6, P1, P3 and F1. The target BS possesses the certificate which is contained in the MAC address of the MSS, the PMK and the nonce generated by the AS. Since a fresh random value is included in the message, the target BS believes that the message is not a replay. Then, the target BS can generate an AK via these keying materials, and verify that the H(AK) received is equal to the H(AK′) generated.

The application of rules T4, T6, P1 and P3 to Msg4, and Assumptions A9 and A12 yields Eqs. (11)–(13). The MSS possesses the ID, nonce, the MAC address of the target BS, and the nonce of the serving BS. Since a fresh random value is included in this message, the MSS believes that the message is fresh. The MSS can generate an AK and verify that the H(AK) received is equal to the H(AK′) generated. If verification is successful, then the MSS and the target BS believe that the AK is shared, and it can be described by Eq. (9).

$$\frac{M \lhd *(*T \mid *N_S \mid *N_T \mid *H(AK) \mid *T - MAC_{Addr})}{M \ni T, N_S, N_T, \#H(AK), T - MAC_{Addr}} \tag{11}$$

$$\frac{M \mid\equiv \#(*N_S, *N_T)}{M \mid\equiv \#(T, N_S, N_T, \#H(AK), T - MAC_{Addr})} \tag{12}$$

$$M \mid\equiv T \mid\equiv M \overset{AK}{\longleftrightarrow} T, \quad T \mid\equiv M \mid\equiv T \overset{AK}{\longleftrightarrow} M \tag{13}$$

Msgs (5), (6) and Eq. (13) yield the following Eqs. (14)–(18), from the application of rules T3, P1, P3

and F1. Since the target BS and the MSS possess the HMAC/CMAC codes, and each others nonces, they can perform mutual authentication via verification of the HMAC/CMAC codes and the TEK, for traffic encryption. If verification is successful, then the target BS and the MSS believe that the TEK is shared, as shown in Eq. (18).

$$\frac{T \triangleleft *\{HMAC/CMAC \mid M \mid T \mid *N_M \mid N_T)}{T \ni HMAC/CMAC, M, N_M} \quad (14)$$

$$\frac{T \mid\equiv \#(N_T)}{T \mid\equiv \#(HMAC/CMAC, M, N_M, N_T)} \quad (15)$$

$$\frac{M \triangleleft *\{*HMAC/CMAC \mid *H(TEK') \mid N_M)}{M \ni HMAC/CMAC, H(TEK'), N_M} \quad (16)$$

$$\frac{M \mid\equiv \#(N_M)}{M \ni \#(HMAC/CMAC, H(TEK'), N_M)} \quad (17)$$

$$T \mid\equiv M \mid\equiv T \overset{TEK}{\longleftrightarrow} M, \quad M \mid\equiv T \mid\equiv M \overset{TEK}{\longleftrightarrow} T \quad (18)$$

Finally, Eqs. (13) and (18) imply that the MSS and the target BS share the AK and TEK, and engage in mutual authentication.

4. Security Analysis

In this section, we analyze our protocol in terms of security requirements. Table 3 shows the comparison of protocols. The security characteristics of IEEE 802.16e depend on handover optimization; Bit #1 and #2. Although the first scenario satisfies all security requirements, it is not suitable for practical handover, because the PKM protocol, which is based on EAP, can increase the handover delay. In [4], for fast handover, the information about the master key is shared between BSs in handover. Hence, mutual authentication and forward/backward secrecy are not guaranteed. In [5], authentication based on pre-authentication is efficient and secure. However, if each ASN can contain one or more base stations, then PMK may be shared by BSs located in the same ASN. In this case, forward/backward secrecy cannot be guaranteed. Our protocol generates a unique PMK and AK without EAP based re-authentication. No BS can derive keys of other BSs, due to the secure PMK and AK, and the one-way property of the Dot16KDF key generation function. In addition, a TEK is generated by both participants, which is more secure. Therefore, our protocol satisfies forward/backward secrecy, as well as mutual authentication.

Table 3 Comparison of protocols.

Protocols		*Mutual Authentication*	*Forward Secrecy*	*Backward Secrecy*
IEEE 802.16e handover optimization	Bit#1=0 Bit#2=0	O	O	O
	Bit#1=1 Bit#2=0	X	X	O
	Bit#1=1 Bit#2=1	X	X	X
[4]		X	X	X
[5]		O	Δ	Δ
Proposed Protocol		O	O	O
O:satisfied, Δ: satisfied depends on option, X:unsatisfied				

5. Conclusion

IEEE 802.16e handover has several vulnerabilities. Via some modifications of the PKM protocol, we tried to overcome the existing vulnerabilities. The proposed protocol provides not only mutual authentication, but also forward/backward secrecy. We proved the correctness and security of the protocol using a GNY logic-based, formal analysis method. In the future, we plan to analyze the performance of the protocol.

References

[1] IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005, "Amendment2 for physical and medium access control layers for combined fixed and mobile operation in licensed bands," Nov. 2005.
[2] IEEE C802.16m-07/029, "Mobility sensitive master key derivation and fast re-authentication for 802.16m," Feb. 2007.
[3] WiMAX Forum, "Mobile WiMAX — Part 1: A technical overview and performance evaluation," Mobile WiMAX Forum White Paper, Feb. 2006.
[4] C. Chang and C. Huang, "Fast and secure mobility for IEEE 802.16e broadband wireless networks," Proc. ICPPW 2007, 2007.
[5] H. Sun, Y. Lin, S. Chen, and Y. Shen, "Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks," Proc. IEEE TENCON 2007, 2007.
[6] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[7] L. Gong, R. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols," Proc. IEEE Symposium on Research in Security and Privacy, pp.234–248, May 1990.
[8] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol.426, pp.18–36, 1990.

Appendix A: Statements

Here, we describe notation used for statements in the paper. Refer to [7], [8] for a detailed description. A basic statement is associated with some property of an equation. Let P and Q range over principals. The basic statements are as follows:
– $P \triangleleft X$: P receives X, possibly after performing some computation such as decryption.
– $P \triangleleft *X$: P receives X, and P never said X.
– $P \ni X$: P possesses equation X.
– $\#(X)$: Equation X is fresh, such that X was not used for an identical purpose prior to the current execution of the protocol.
– $P \mid\equiv X$: P believes that statement C is valid.
– $P \mid\equiv P \overset{S}{\longleftrightarrow} Q$: P believes that S is a suitable secret for P and Q. They may properly use it to mutually prove their identity. They may also use it as a key, or derive a key from it, to communicate.
– C1, C2: Conjunction.

Appendix B: Logical Postulates

In this section, we introduce the logical postulates underpinning reasoning. There are five categories of postulates.

We describe the characteristics of each category and present representative postulates. For the complete list of postulates, refer to [7], [8] for a detailed description.

Being-Told Rules

– (T1) $\frac{P \triangleleft *X}{P \triangleleft X}$: P receives an equation which he did not previously send in the current execution.

– (T2) $\frac{P \triangleleft (X, Y)}{P \triangleleft X}$: Being-told an equation implies being told of each of its concatenated components.

– (T3) $\frac{P \triangleleft \{X\}_K,\ P \ni K}{P \triangleleft X}$: if P receives an equation encrypted with a key P possesses, then P is also considered to have been told the decrypted contents of that equation.

– (T4) $\frac{P \triangleleft \{X\}_{+K},\ P \ni -K}{P \triangleleft X}$: If P receives an equation encrypted with a public key, and P possesses the corresponding private key, then P is also considered to have been told the decrypted contents of that equation.

– (T6) $\frac{P \triangleleft \{X\}_{-K},\ P \ni +K}{P \triangleleft X}$: If P receives an equation encrypted with a private key, and P possesses the corresponding public key, then P is also considered to have been told the decrypted contents of that equation.

Possession Rules

– (P1) $\frac{P \triangleleft X}{P \ni X}$: A principal is capable of possessing anything he is told.

– (P3) $\frac{P \ni (X, Y)}{P \ni X}$: If P possesses an equation, then P is capable of possessing any of the concatenated components of that equation.

Freshness Rules

– (F1) $\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y), P \mid\equiv \#(F(X))}$: If P believes a formal X is fresh, then P believes that any equation of which X is a component is fresh, and a one-to-one function F of X is fresh, and can be computed in real-time.